Security needs spawn services
Managed detection services growing in popularity.
Byline: ELLEN MESSMER
Journal: Network World Page Number: 1
Publication Date: April 03, 2000
Word Count: 733 Line Count: 75
Text:

Companies installing **intrusion**-detection software to protect their networks are faced with this practical question: Do we have the skills and time to keep the round-the-clock vigils the software requires?The alternative is going to an outside firm that offers a managed security service that can identify denial-of-service attacks or other threats. This week, Internet Security Systems (ISS), which specializes in scanning software, and start-up **Counterpane** Internet Security, will each begin offering its own style of managed **intrusion**-detection services, boosting choice in an underserved area of security.Although companies such as UUNET, AT&T and Exodus offer managed firewall services, only a few providers, including Pilot Network Services, have ventured to take on what is arguably the bigger challenge. And that's **monitoring** the customer's internal servers and network traffic, where some type of **intrusion** -detection sensors must be deployed to determine if systems are under attack.Unlike the new offerings from ISS and **Counterpane**, the Pilot **Network** Services model requires firms to house equipment at a Pilot data center and connect to it by a private line."We're doing a security **monitoring** service by putting a probe on the customer's network to accept audit data from a wide range of devices," says Bruce Schneier, **Counterpane**'s chief technology officer. Schneier, a leading cryptographer, started the company with $7 million in venture-capital funding from Bessemer Ventures and other firms.**Counterpane** 's Linux-based "black box" sensor captures syslog and audit outputs from Windows NT, Solaris and Linux servers; routers; security gear such as Check Point Software and Cisco Pix firewalls; plus ISS and Tripwire **intrusion**-detection software.The **Counterpane** box regularly transmits the network activity output in encrypted form to **Counterpane** 's data centers in Mountain View, Calif., or Chantilly, Va., where it is **monitored** around the clock. "Embedded in this data are the footprints of attacks, and our analysts are trained to understand them," Schneier says, adding **Counterpane** staffers advise corporations on how to combat threats but do not make changes to the corporation's equipment.Santa Clara service provider Conxion, which specializes in hosting business-to-business applications for customers including Visa International, has started using the **Counterpane** service. "All our critical infrastructure devices report to the **Counterpane** device," says Conxion security director Mark Kadrich. "We have more than 20 firewalls, we use all the ISS **intrusion**-detection software, and it's hard to find qualified people to analyze this mind-numbing output."Although some may argue that outsourcing network security management is an unacceptable risk, Kadrich - who requires everyone on his staff to earn the coveted CISSP security certification - argues otherwise. "Security needs to be results-based, and those unwilling to outsource don't really understand the problem," he says.**Counterpane** says its service costs about $12,000 per month.ISS, which holds about 60% of the market for **intrusion** -detection software according to market research firm IDC, has also recognized the pent-up demand for outsourcing help."We have 5,500 customers today, mostly larger firms, but there are literally millions of businesses drawn to the Internet for business-to-consumer or business-to-business e-commerce," says ISS CEO Thomas Noonan. "For many of them, security is important but misunderstood, and many have small IT departments."ISS, which offers six products for network and application scanning and vulnerability assessment, has now developed a Managed Security

Services platform. The offering, based on technology obtained through the acquisition of a company called Netrex, will enable ISPs and telecommunications firms to provide outsourced security **monitoring.** Customers will have to deploy the ISS SafeSuite **intrusion-detection** sensor on their sites to get the security **monitoring** service.Under the plan, ISS will supply security experts to work in operation centers at ISPs and telecom firms. These experts will **monitor** corporate routers, provide Web-content filtering, and watch Check Point and WatchGuard firewalls, as well as the ISS **intrusion**-detection software.According to Noonan, Ameritech, AT&T, Embratel, US West, BellSouth, NTT, Savvis and other service providers around the world have signed agreements to use the ISS Managed Security Services platform. Corporate customers for this so-called ePatrol Service will be given remote access to the same security view of their networks as the ISPs and telecom firms will have, Noonan says.Some companies are already sold on managed security services.ContiGroup Companies, formerly Continental Grain, has used the Pilot managed service for **intrusion** detection for about a year, installing the corporate firewall at Pilot. "We didn't have the staff with the expertise for this, and the relationship with Pilot has worked well to fight viruses and hacking attempts," says Bill Clark, Internet service manager.**Counterpane:** www.counter pane.com; ISS: www.iss.net
?